為請求方訪問配置電腦雙因素身份驗證

目錄

簡介

本文檔介紹使用電腦和dot1x身份驗證配置雙因素身份驗證所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身份服務引擎的配置
- Cisco Catalyst的配置
- IEEE802.1X

採用元件

- 身分辨識服務引擎虛擬3.3修補程式1
- C1000-48FP-4G-L 15.2(7)E9

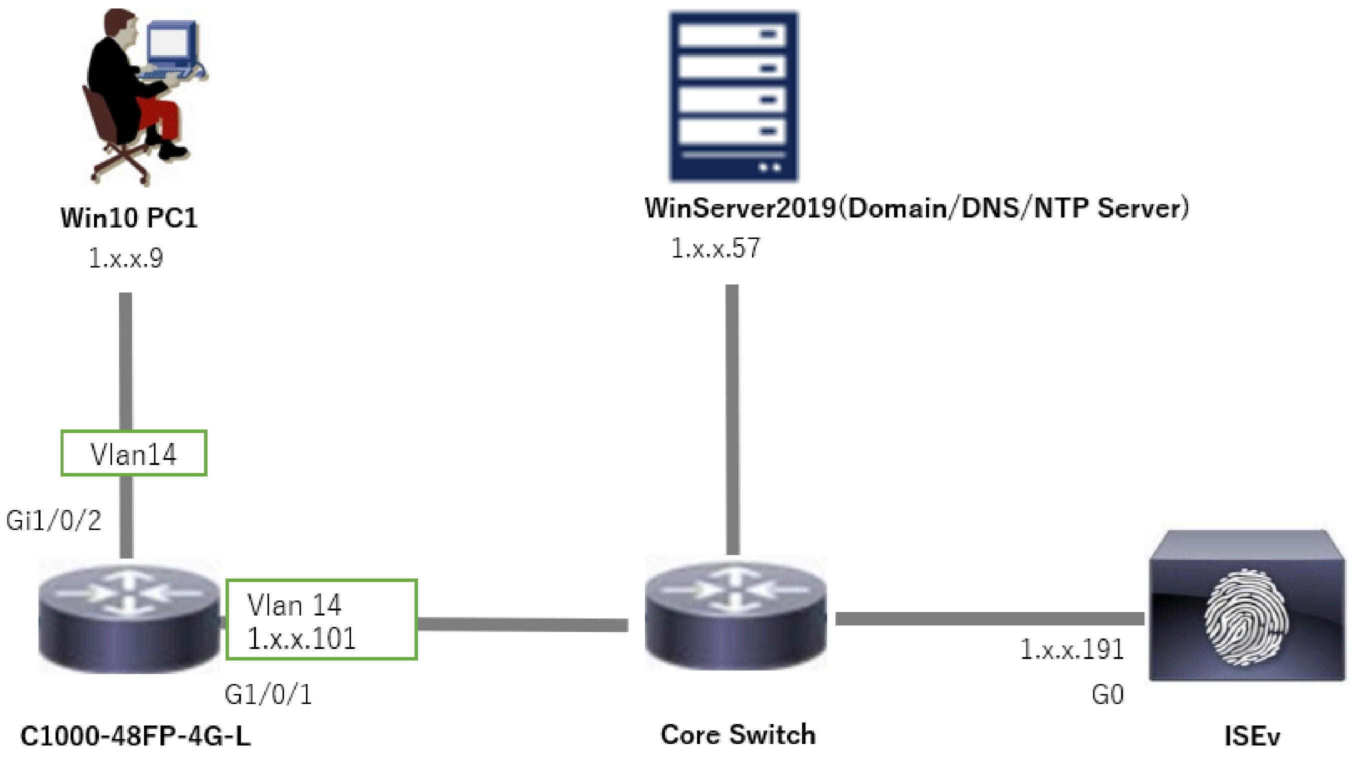
- Windows Server 2019

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表

下圖顯示本文檔示例中使用的拓撲。

在Windows Server 2019上配置的域名是ad.rem-xxx.com，本文檔中用作示例。



網路圖表

背景資訊

電腦身份驗證是驗證尋求訪問網路或系統的裝置的身份的安全過程。使用者身份驗證基於使用者名稱和密碼等身份證明來驗證個人身份，而電腦身份驗證則不同，它側重於驗證裝置本身。這通常使用裝置特有的數位證書或安全金鑰來完成。

透過同時使用電腦和使用者身份驗證，組織可以確保只有獲得授權的裝置和使用者才能訪問其網路，從而提供更加安全的環境。此雙因素身份驗證方法對於保護敏感資訊和遵守嚴格的法規標準特別有用。

組態

C1000中的配置

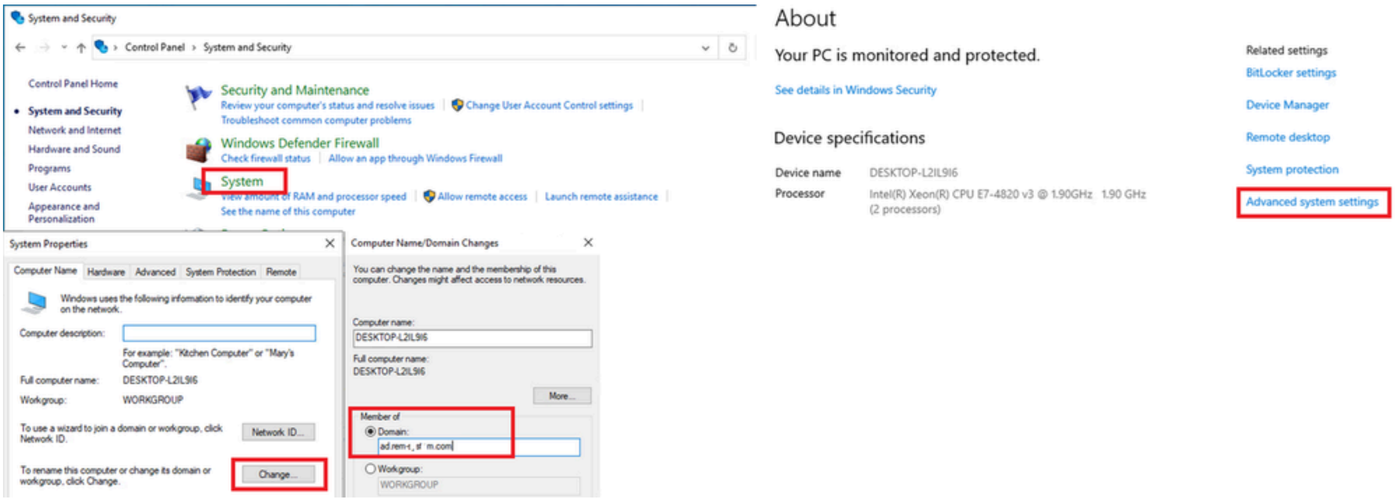
這是C1000 CLI中的最小配置。

```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
key cisco123

aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Windows PC中的配置

步驟 1.將PC增加到AD域

導航到控制台>系統和安全，點選系統，然後點選高級系統設定。在「System Properties」窗口中，按一下Change，選擇Domain並輸入域名。


System and Security

Control Panel › System and Security

Control Panel Home
- System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name: DESKTOP-L2IL9I6
Processor: Intel(R) Xeon(R) CPU E7-4820 v3 @ 1.90GHz 1.90 GHz (2 processors)

Related settings
BitLocker settings
Device Manager
Remote desktop
System protection
Advanced system settings

System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Windows uses the following information to identify your computer on the network.

Computer description:
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name: DESKTOP-L2IL9I6
Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID. [Network ID...]

To rename this computer or change its domain or workgroup, click Change. [Change...]

Computer Name/Domain Changes

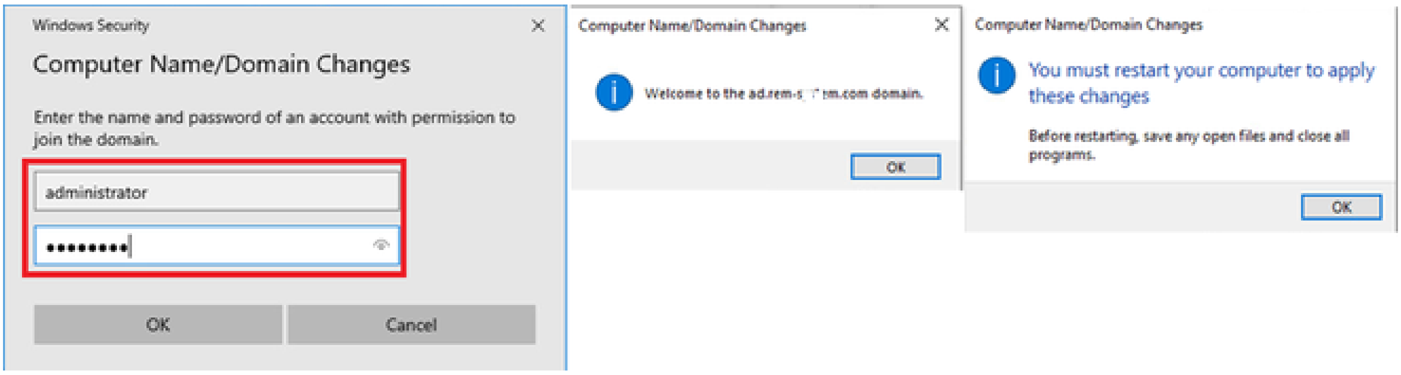
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: DESKTOP-L2IL9I6
Full computer name: DESKTOP-L2IL9I6
[More...]

Member of
● Domain: ad.rem-s m.com
○ Workgroup: WORKGROUP

將PC增加到AD域

在「Windows安全性」視窗中，輸入網域伺服器的使用者名稱和密碼。


Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

administrator

••••••••

[OK] [Cancel]

Computer Name/Domain Changes

Welcome to the ad.rem-s m.com domain.

[OK]

Computer Name/Domain Changes

You must restart your computer to apply these changes

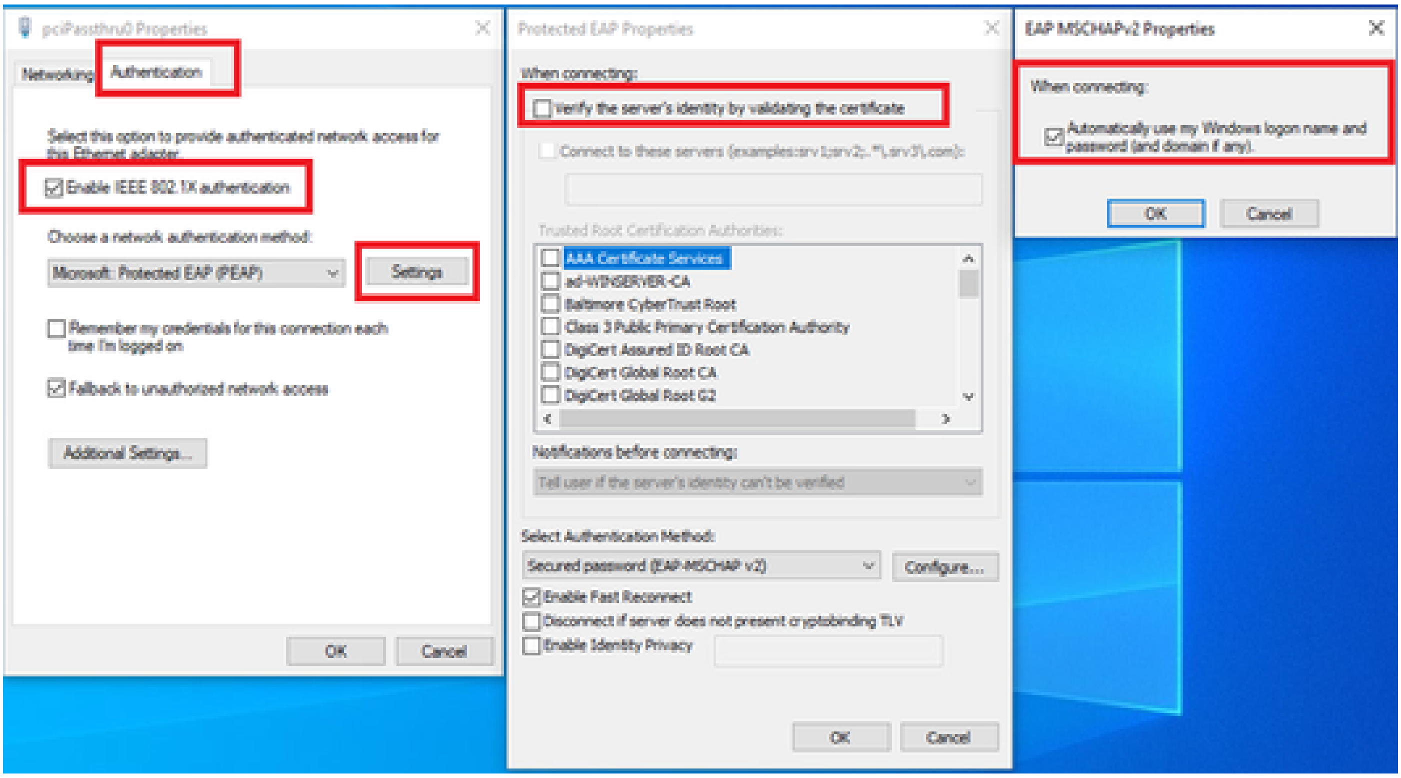
Before restarting, save any open files and close all programs.

[OK]

輸入使用者名稱和密碼

步驟 2.配置使用者身份驗證

導航到身份驗證，選中啟用IEEE 802.1X身份驗證。 在「受保護的EAP屬性」窗口中按一下設定，取消選中驗證證書以驗證伺服器的身份，然後按一下配置。在「EAP MSCHAPv2 Properties」窗口中，選中Automatically use my Windows logon name and password(and domain if any)，使用在Windows電腦登入期間輸入的使用者名稱進行使用者身份驗證。



pciPassthru0 Properties

Networking | Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

☐ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Additional Settings...

OK | Cancel

Protected EAP Properties

When connecting:

☐ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

☐ AAA Certificate Services
☐ ad-WINSERVER-CA
☐ Baltimore CyberTrust Root
☐ Class 3 Public Primary Certification Authority
☐ DigiCert Assured ID Root CA
☐ DigiCert Global Root CA
☐ DigiCert Global Root G2

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

☑ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK | Cancel

EAP MSCHAPv2 Properties

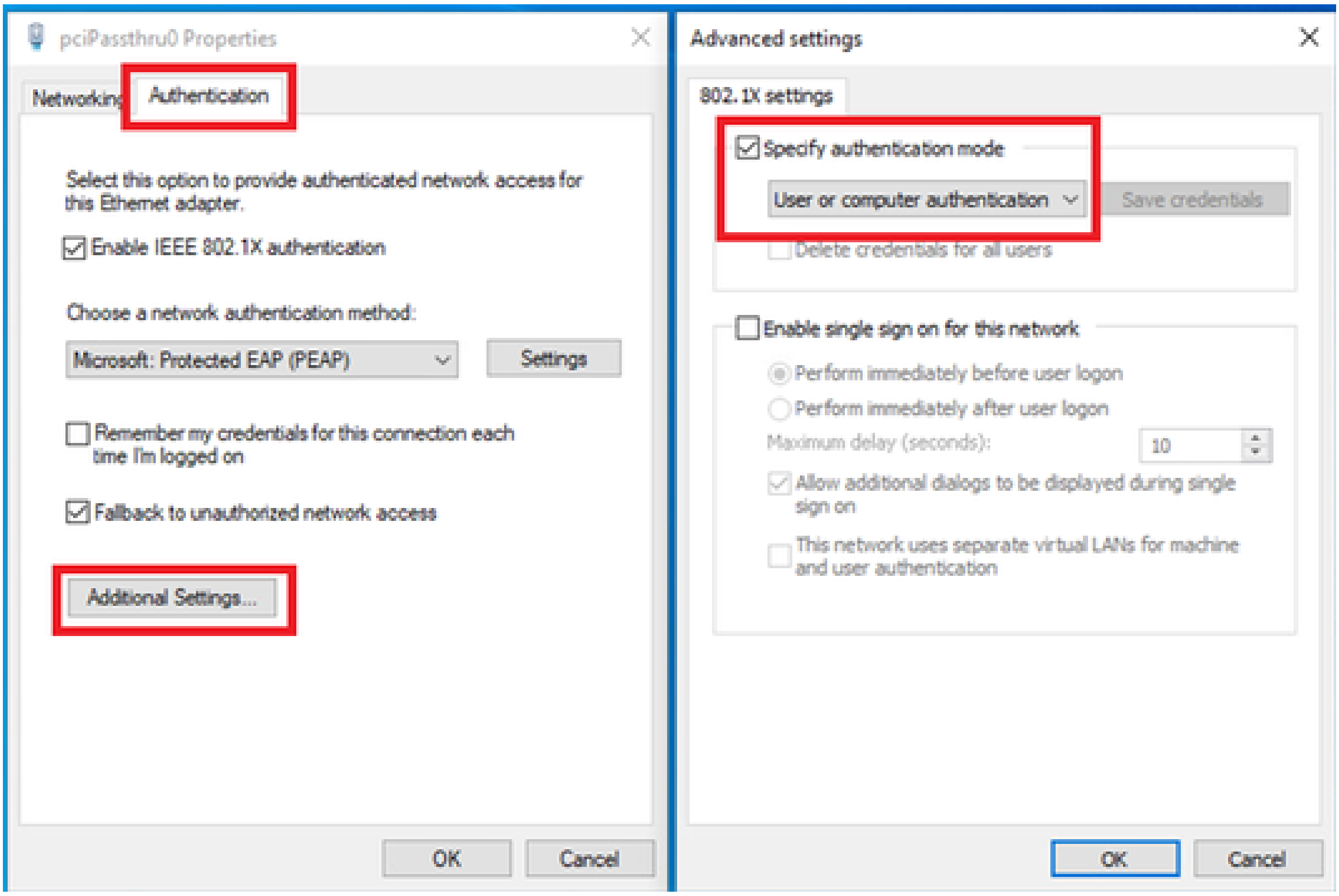
When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

啟用使用者身份驗證

導航到身份驗證，選中其他設定。從下拉選單中選擇User or computer authentication。



pciPassthru0 Properties

Networking | Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

☐ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Additional Settings...

OK | Cancel

Advanced settings

802.1X settings

☑ Specify authentication mode

User or computer authentication | Save credentials

☐ Delete credentials for all users

☐ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication

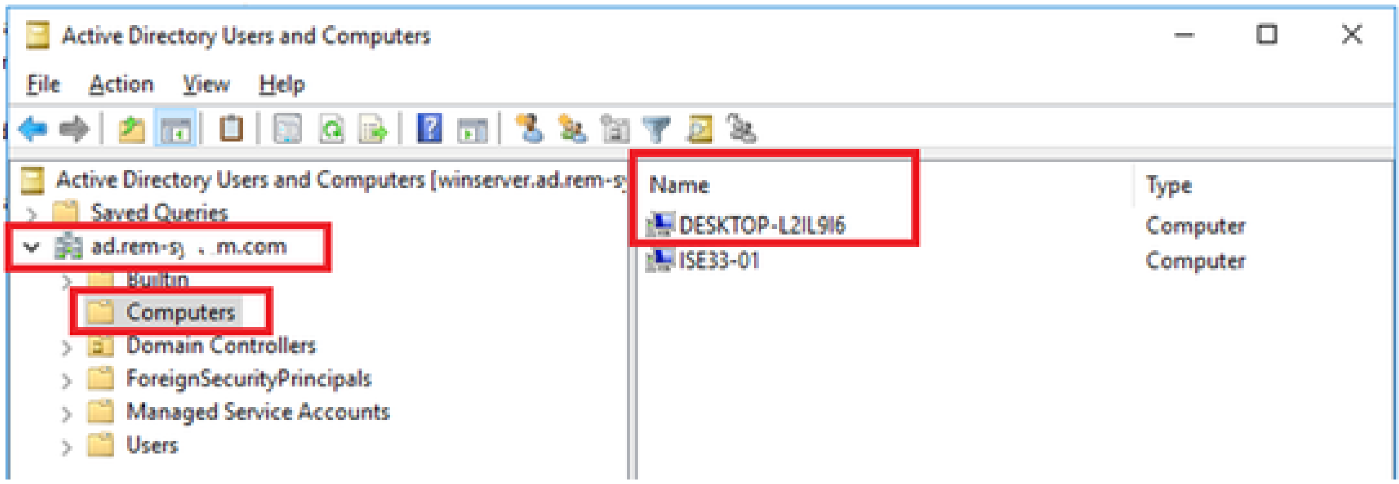
OK Cancel

指定驗證模式

Windows Server中的配置

步驟 1.確認網域電腦

導航到Active Directory使用者和電腦，按一下電腦。確認Win10 PC1已列在域中。

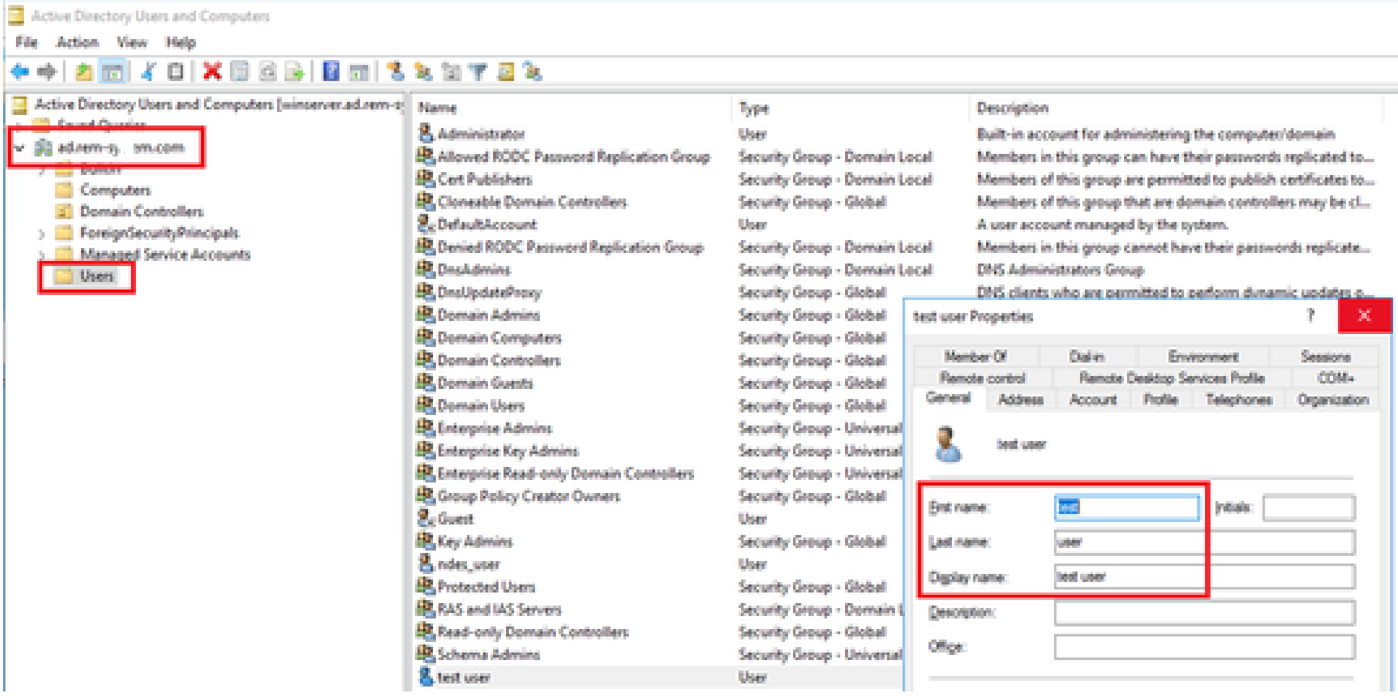

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [winserver.ad.rem-sy
Saved Queries
ad.rem-s)　.m.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users

Name	Type
DESKTOP-L2IL9I6	Computer
ISE33-01	Computer

確認網域電腦

步驟 2.新增網域使用者

導航到Active Directory使用者和電腦，按一下使用者。將testuser新增為網域使用者。

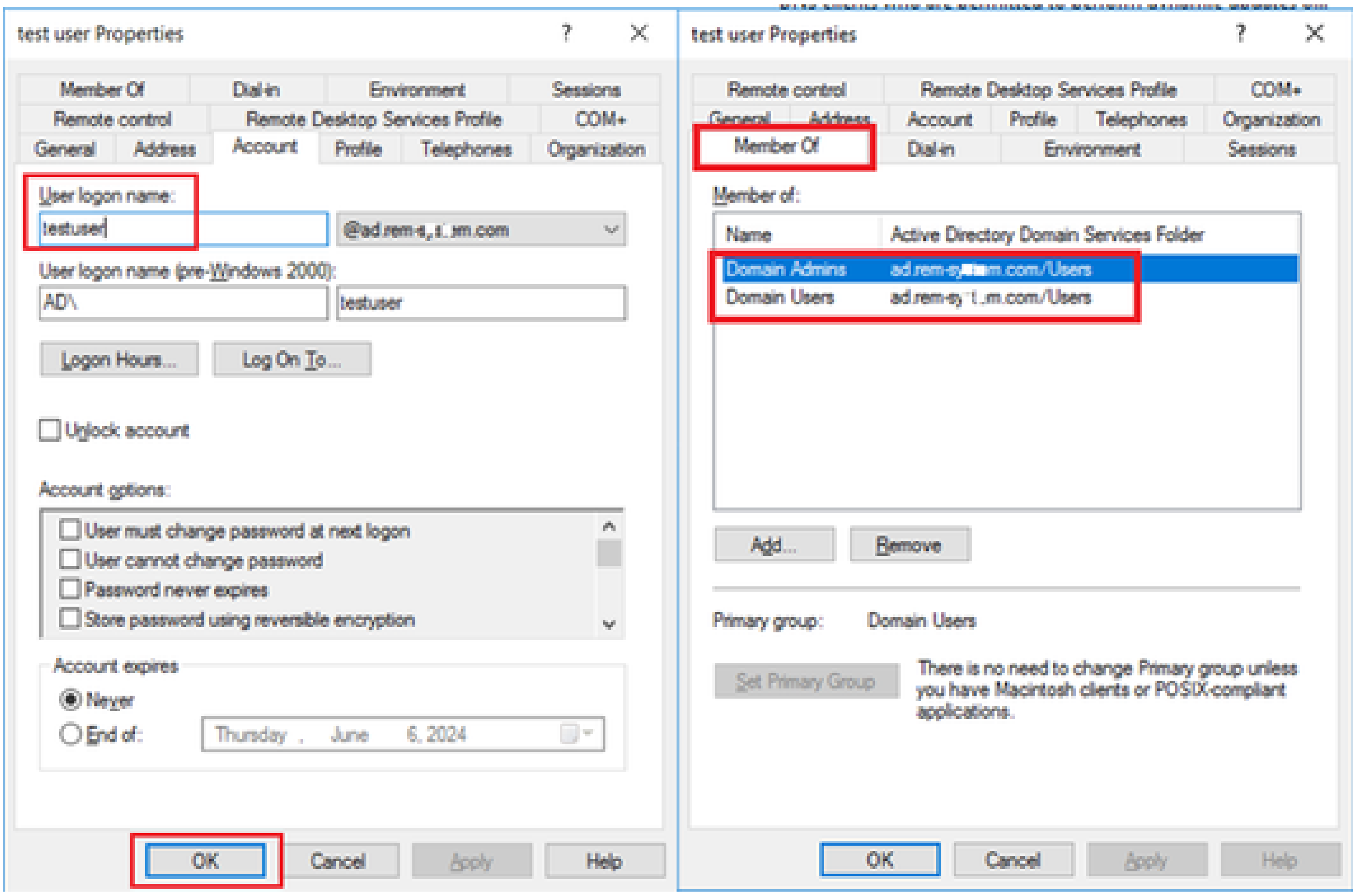


Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to...
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates to...
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may be cl...
DefaultAccount	User	A user account managed by the system.
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicate...
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates o...
Domain Admins	Security Group - Global	
Domain Computers	Security Group - Global	
Domain Controllers	Security Group - Global	
Domain Guests	Security Group - Global	
Domain Users	Security Group - Global	
Enterprise Admins	Security Group - Universal	
Enterprise Key Admins	Security Group - Universal	
Enterprise Read-only Domain Controllers	Security Group - Universal	
Group Policy Creator Owners	Security Group - Global	
Guest	User	
Key Admins	Security Group - Global	
ndes_user	User	
Protected Users	Security Group - Global	
RAS and IAS Servers	Security Group - Domain L	
Read-only Domain Controllers	Security Group - Global	
Schema Admins	Security Group - Universal	
test user	User	

First name: test
Initials:
Last name: user
Display name: test user
Description:
Office:

新增網域使用者

將域使用者增加到域管理員和域使用者的成員。



User logon name:

testuser @ad.rem-s[redacted]m.com

User logon name (pre-Windows 2000):

AD\ testuser

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Thursday , June 6, 2024

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	ad.rem-sy[redacted]m.com/Users
Domain Users	ad.rem-s[redacted]m.com/Users

Primary group: Domain Users

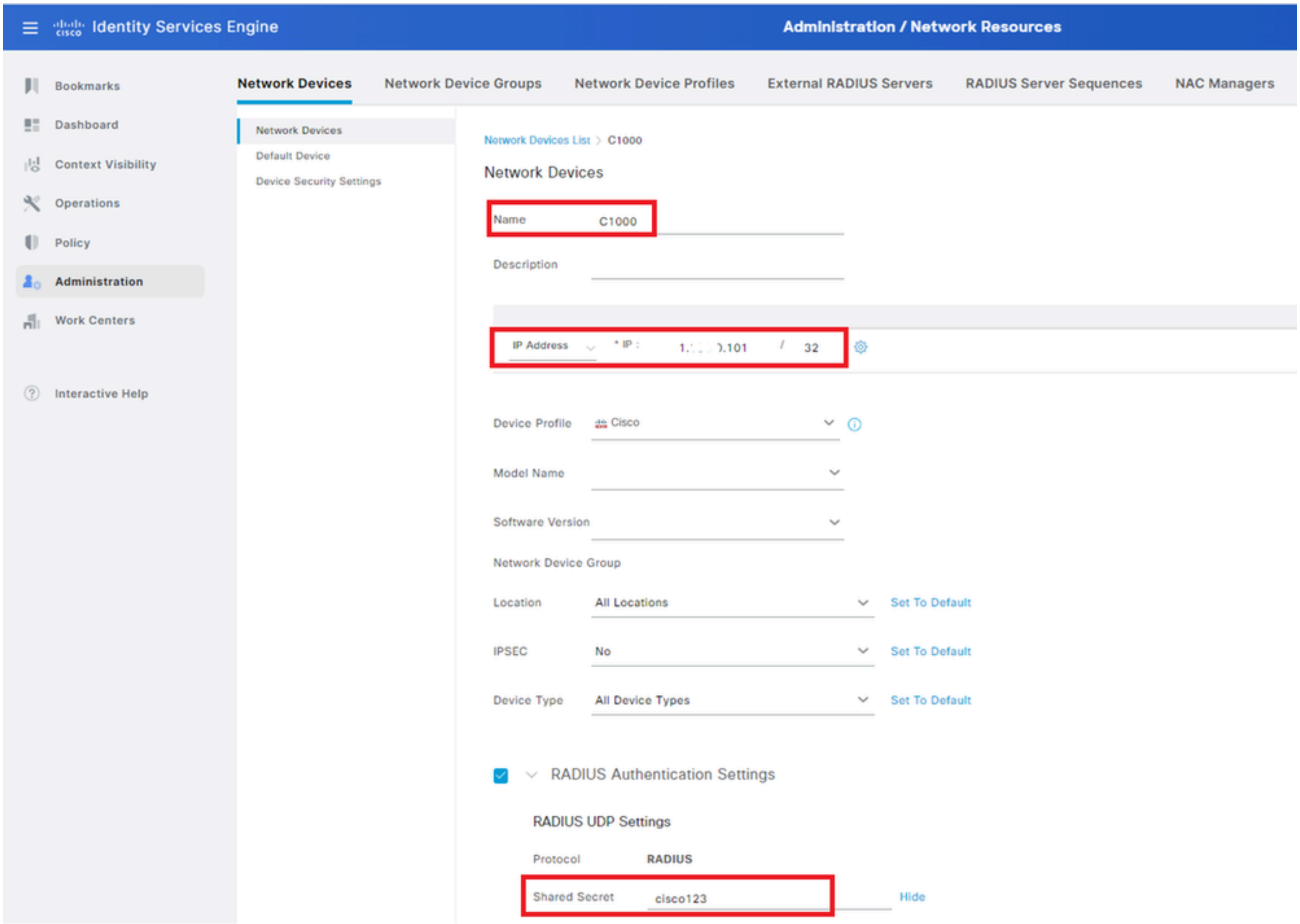
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

域管理員和域使用者

ISE中的配置

步驟 1.增加裝置

導航到管理>網路裝置，點選增加按鈕增加C1000裝置。



Name C1000

Description

IP Address * IP : 1.[redacted].101 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

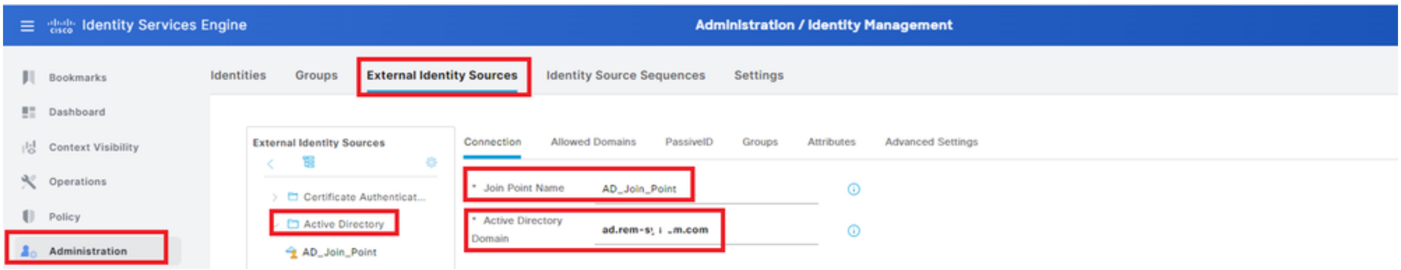
Shared Secret cisco123 Hide

增加裝置

步驟 2.新增Active Directory

導航到管理>外部身份源> Active Directory，點選連線頁籤，將Active Directory增加到ISE。

- 連線點名稱：AD_Join_Point
- Active Directory域： ad.rem-xxx.com

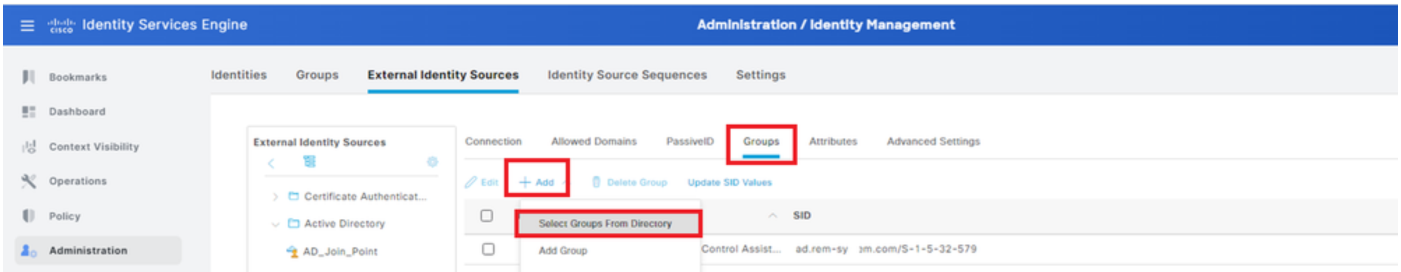


* Join Point Name AD_Join_Point

* Active Directory Domain ad.rem-s[redacted]m.com

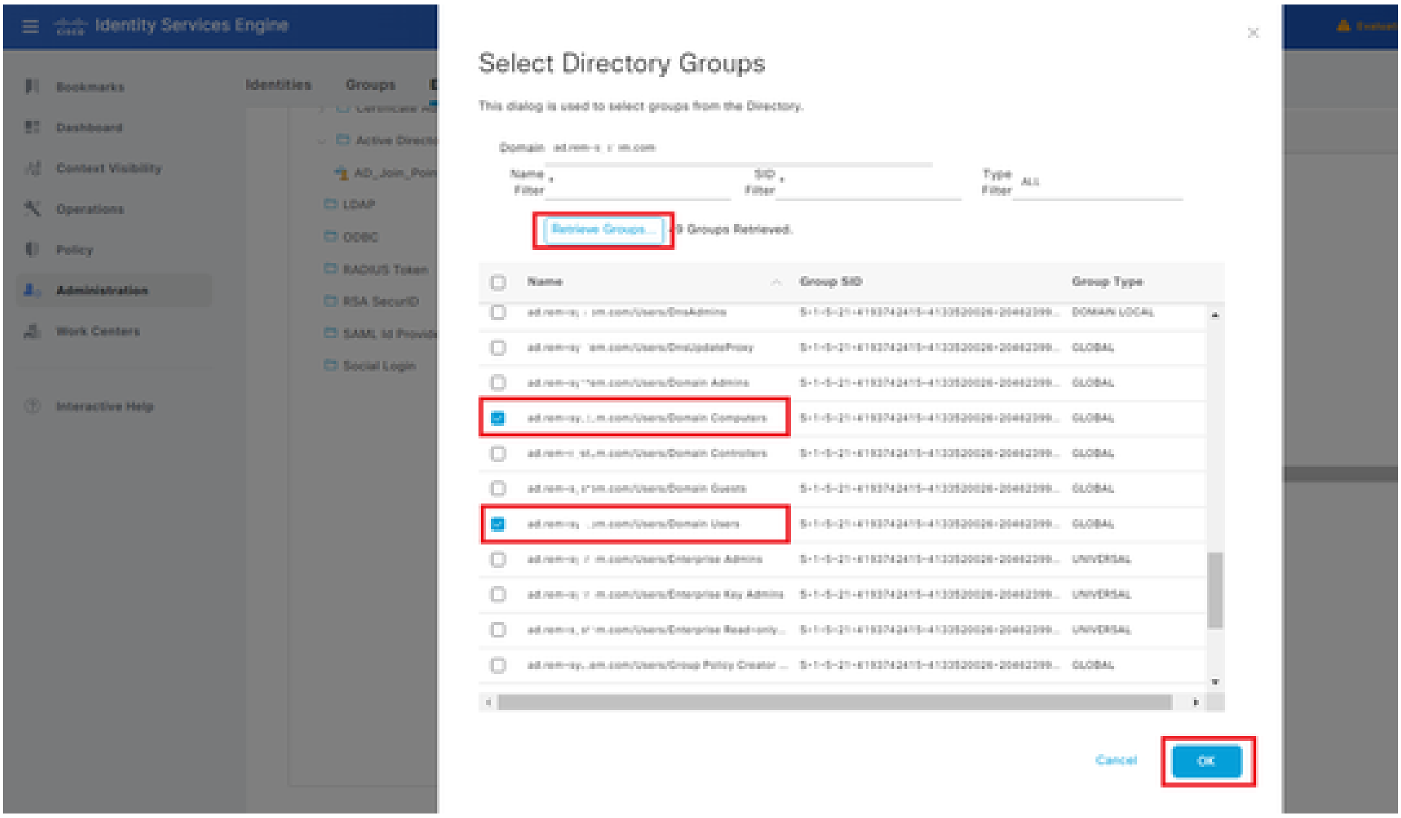
新增Active Directory

導航到組頁籤，從下拉選單中選擇選擇目錄中的組。



從目錄選取群組

從下拉選單中選擇Retrieve Groups。選中ad.rem-xxx.com/Users/Domain Computers和ad.rem-xxx.com/Users/Domain Users，然後按一下OK。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain ad.rem-s r m.com

Name Filter *

SID Filter *

Type Filter ALL

Retrieve Groups... 49 Groups Retrieved.

□	Name	Group SID	Group Type
□	ad.rem-sy · m.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-sy m.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy m.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-sy m.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-s m.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-s m.com/Users/Domain Guests	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-sy m.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-sy m.com/Users/Enterprise Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
□	ad.rem-sy m.com/Users/Enterprise Key Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
□	ad.rem-s m.com/Users/Enterprise Read-only...	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
□	ad.rem-sy m.com/Users/Group Policy Creator ...	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

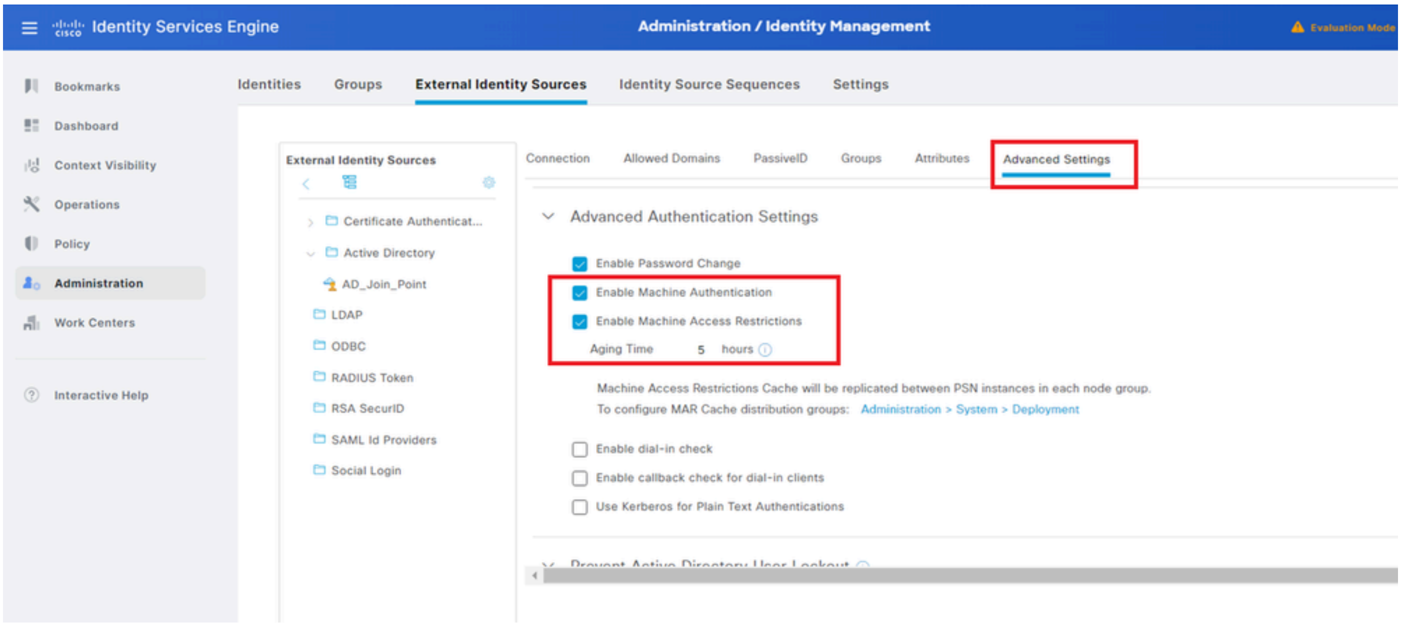
增加域電腦和使用者

步驟 3.確認電腦身份驗證設定

導航到高級設定頁籤，確認電腦身份驗證的設定。

- 啟用電腦身份驗證：啟用電腦身份驗證
- 啟用電腦存取限制：在授權前結合使用者和電腦驗證

註：有效老化時間範圍為1至8760。



Advanced Authentication Settings

☑ Enable Password Change

☑ Enable Machine Authentication

☑ Enable Machine Access Restrictions

Aging Time 5 hours

Machine Access Restrictions Cache will be replicated between PSN instances in each node group.
To configure MAR Cache distribution groups: Administration > System > Deployment

☐ Enable dial-in check

☐ Enable callback check for dial-in clients

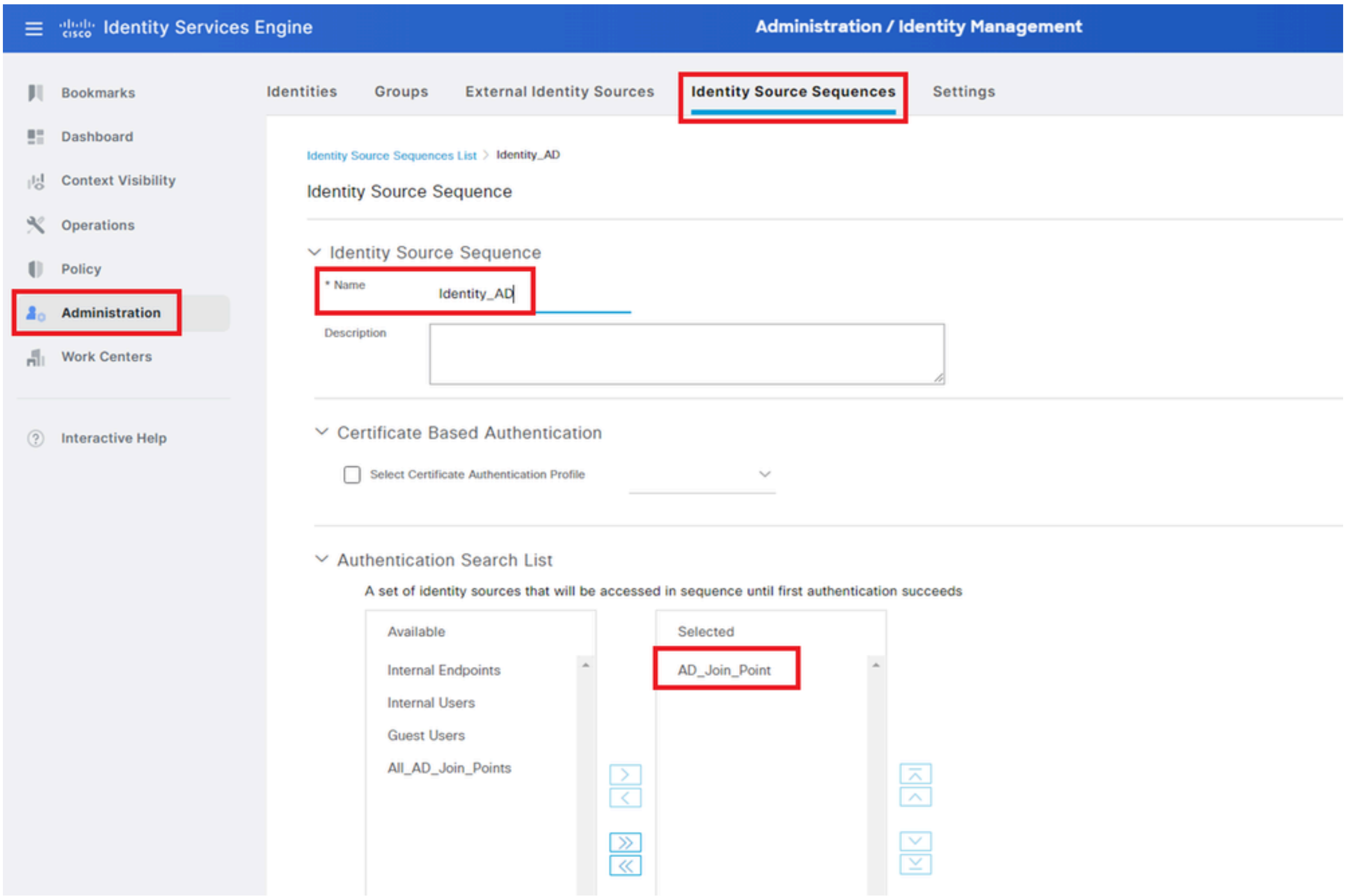
☐ Use Kerberos for Plain Text Authentications

Prevent Active Directory User Lockout

步驟 4.增加身份源序列

導航到管理>身份源序列，增加身份源序列。

- 名稱：Identity_AD
- 身份驗證搜尋清單：AD_Join_Point



* Name: Identity_AD

Description

□ Select Certificate Authentication Profile

A set of identity sources that will be accessed in sequence until first authentication succeeds

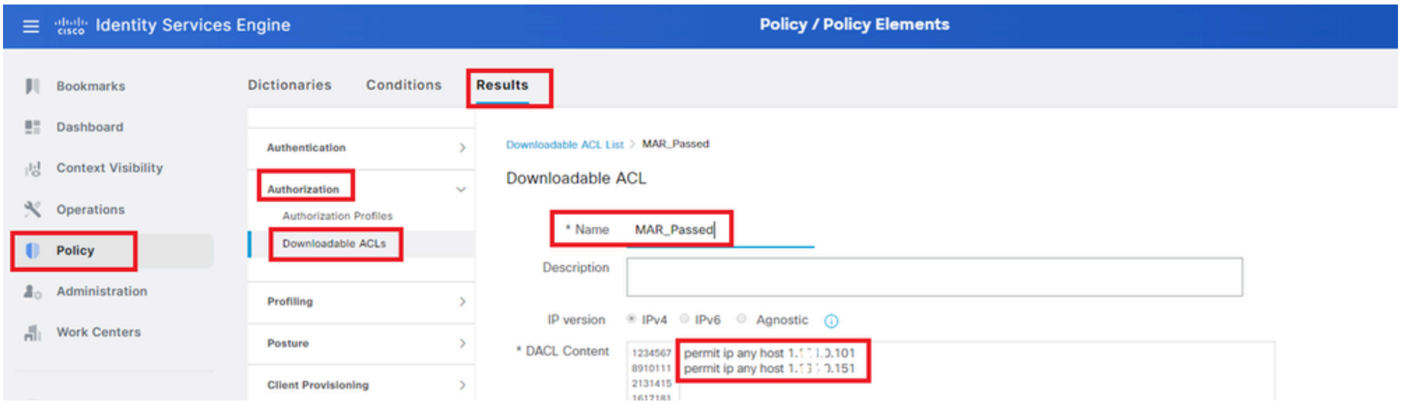
Selected: AD_Join_Point

增加身份源序列

步驟 5.增加DACL和授權配置檔案

導航到策略>結果>授權>可下載ACL，增加DACL。

- 名稱：MAR_Passed
- DACL內容：permit ip any host 1.x.x.101和permit ip any host 1.x.x.105



Downloadable ACL

* Name MAR_Passed

Description

IP version ● IPv4 ○ IPv6 ○ Agnostic

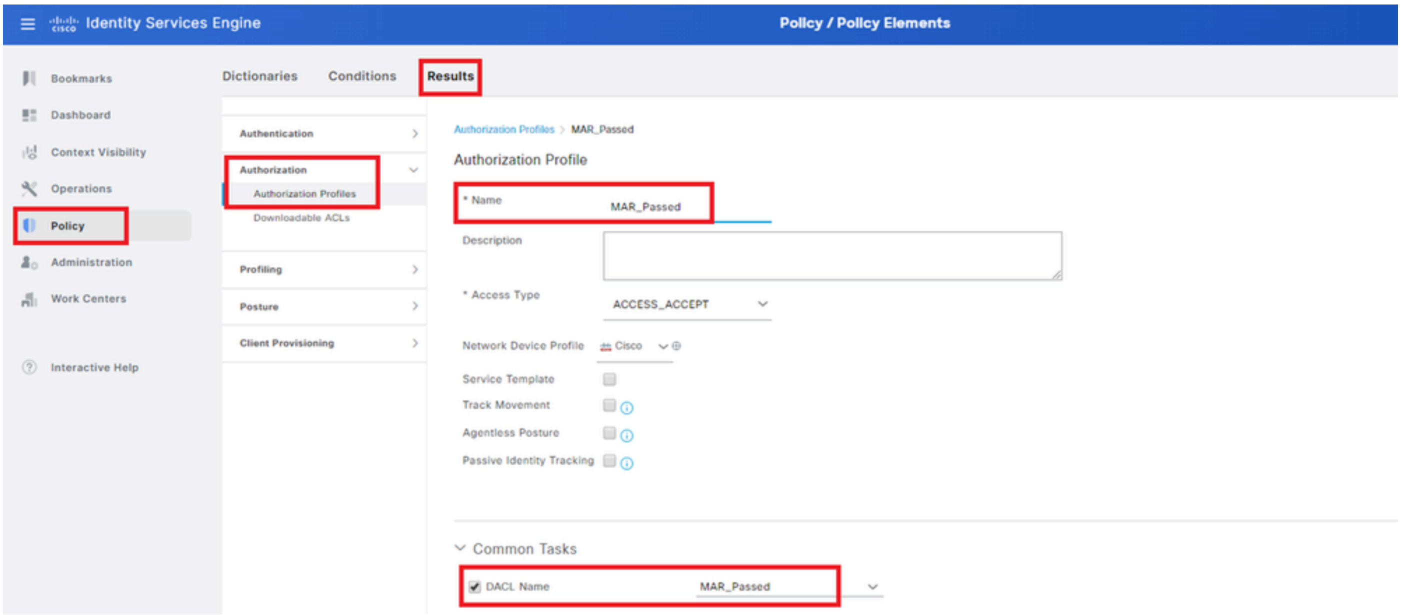
* DACL Content

```
permit ip any host 1.[redacted].0.101
permit ip any host 1.[redacted].0.151
```

增加DACL

導航到策略>結果>授權>授權配置檔案，增加授權配置檔案。

- 名稱：MAR_Passed
- DACL名稱：MAR_Passed



Authorization Profile

* Name MAR_Passed

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

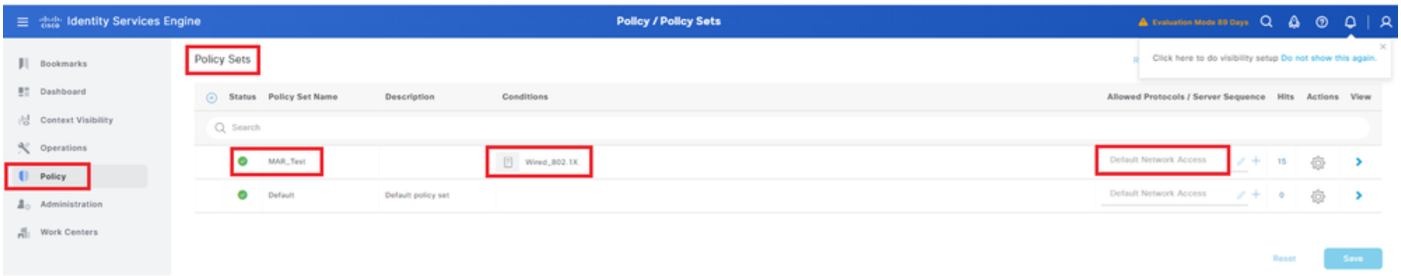
☑ DACL Name MAR_Passed

增加授權配置檔案

步驟 6.增加策略集

導航到策略>策略集，點選+ 增加策略集。

- 原則集名稱：MAR_Test
- 條件：Wired_802.1X
- 允許的協定/伺服器序列：預設網路訪問



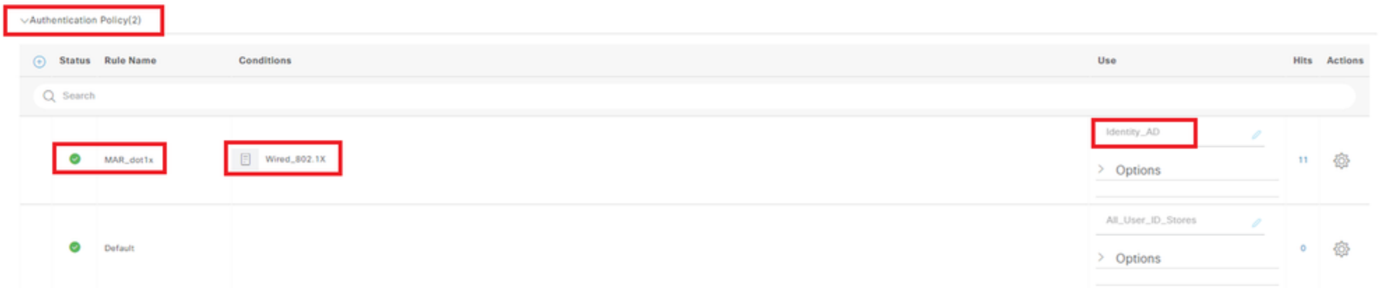
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	MAR_Test		Wired_802.1X	Default Network Access	15	⚙	>
●	Default	Default policy set		Default Network Access	0	⚙	>

增加策略集

步驟 7.增加身份驗證策略

導航到策略集，點選MAR_Test以增加身份驗證策略。

- 規則名稱：MAR_dot1x
- 條件：Wired_802.1X
- 使用：Identity_AD



Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAR_dot1x	Wired_802.1X	Identity_AD Options	11	⚙
✓	Default		All_User_ID_Stores Options	0	⚙

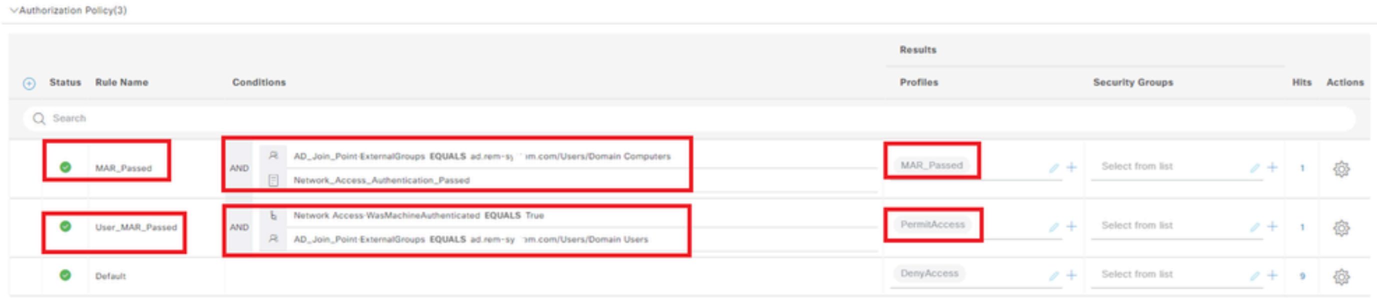
增加身份驗證策略

步驟 8.增加授權策略

導航到策略集，點選MAR_Test以增加授權策略。

- 規則名稱：MAR_Passed
- 條件： AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- 結果：MAR_Passed

- 規則名稱：User_MAR_Passed
- 條件：網路訪問·WasMachineAuthenticated 等於True 且AD_Join_Point·ExternalGroups 等於 ad.rem-xxx.com/Users/Domain使用者
- 結果：PermitAccess



Authorization Policy(3)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	MAR_Passed	AND AD_Join_Point·ExternalGroups EQUALS ad.rem-sy m.com/Users/Domain Computers Network_Access_Authentication_Passed	MAR_Passed	Select from list	1	⚙
✓	User_MAR_Passed	AND Network Access·WasMachineAuthenticated EQUALS True AD_Join_Point·ExternalGroups EQUALS ad.rem-sy m.com/Users/Domain Users	PermitAccess	Select from list	1	⚙
✓	Default		DenyAccess	Select from list	9	⚙

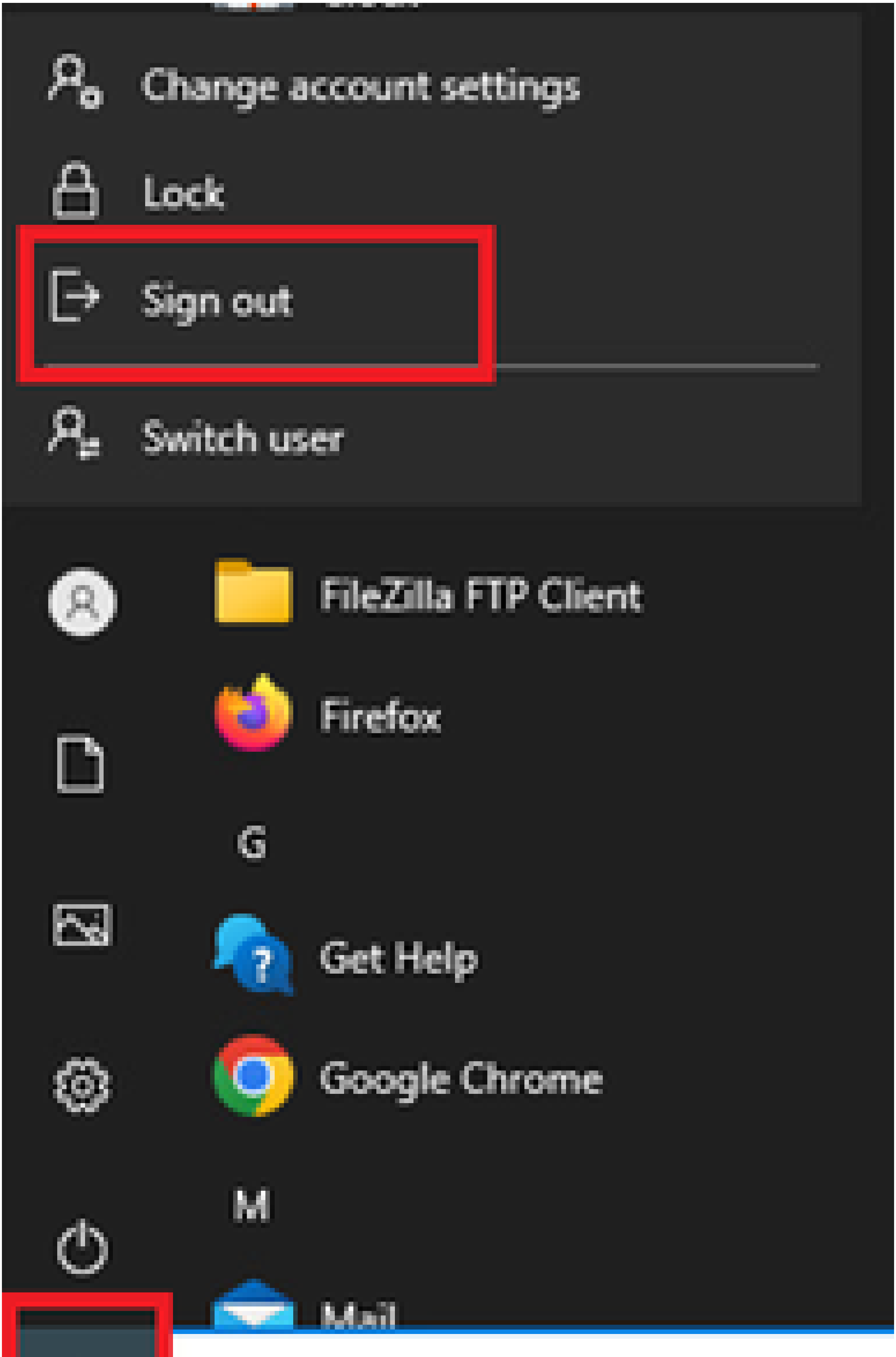
增加授權策略

驗證

模式1.電腦身份驗證和使用者身份驗證

步驟 1.登出Windows PC

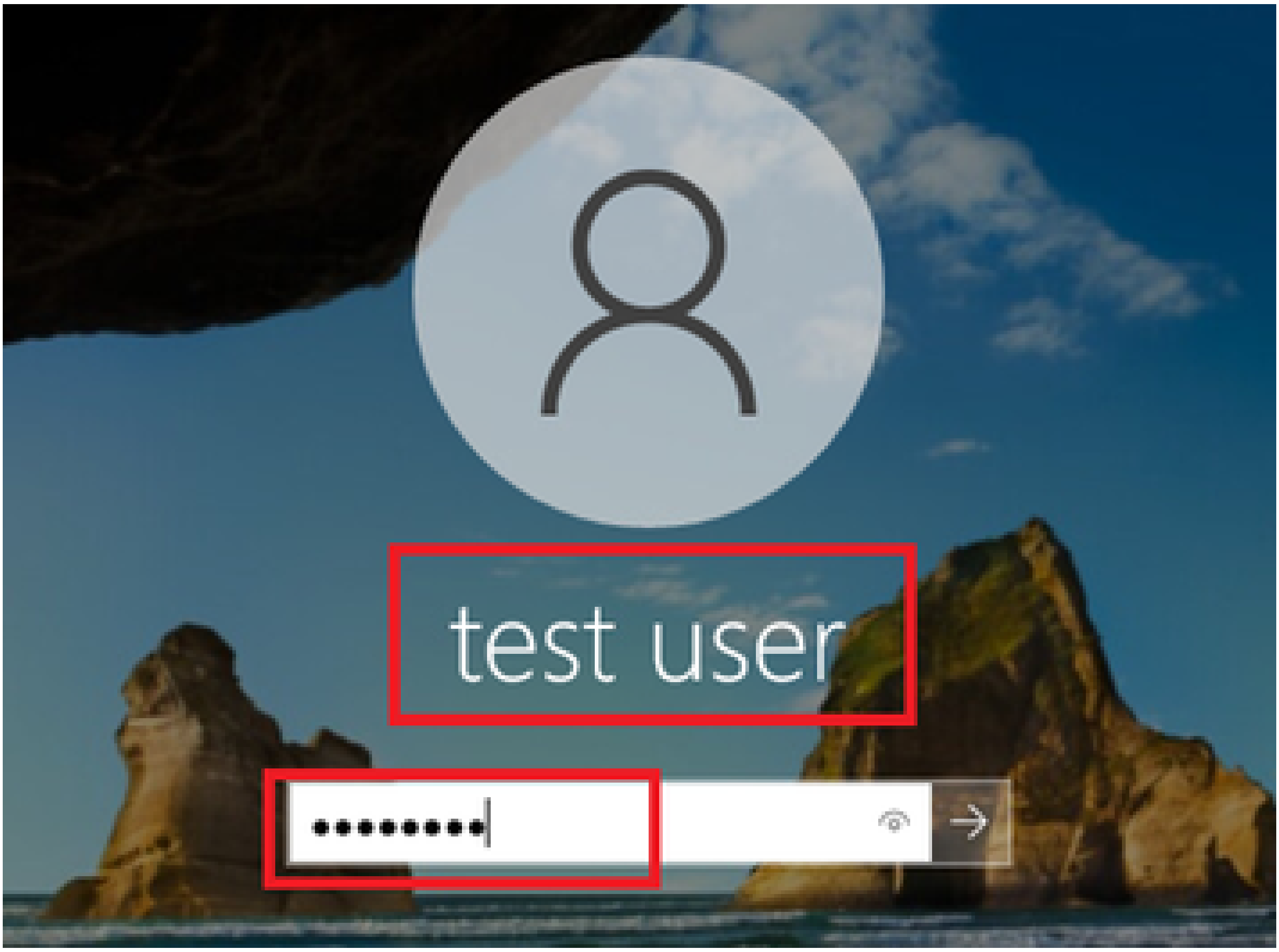
按一下Win10 PC1中的Sign out按鈕以觸發電腦身份驗證。


Change account settings
Lock
Sign out
Switch user
FileZilla FTP Client
Firefox
G
Get Help
Google Chrome
M
Mail

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:

host/DESKTOP-L2IL9I6.ad.rem-xxx.com


Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 5s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003C
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success
```

步驟 3.登入Windows PC

登入Win10 PC1，輸入使用者名稱和密碼以觸發使用者身份驗證。



登入*Windows PC*

步驟 4.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/2 details命令以確認C1000中的使用者身份驗證會話。

<#root>

Switch#

```
show authentication sessions interface GigabitEthernet1/0/2 details
```

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

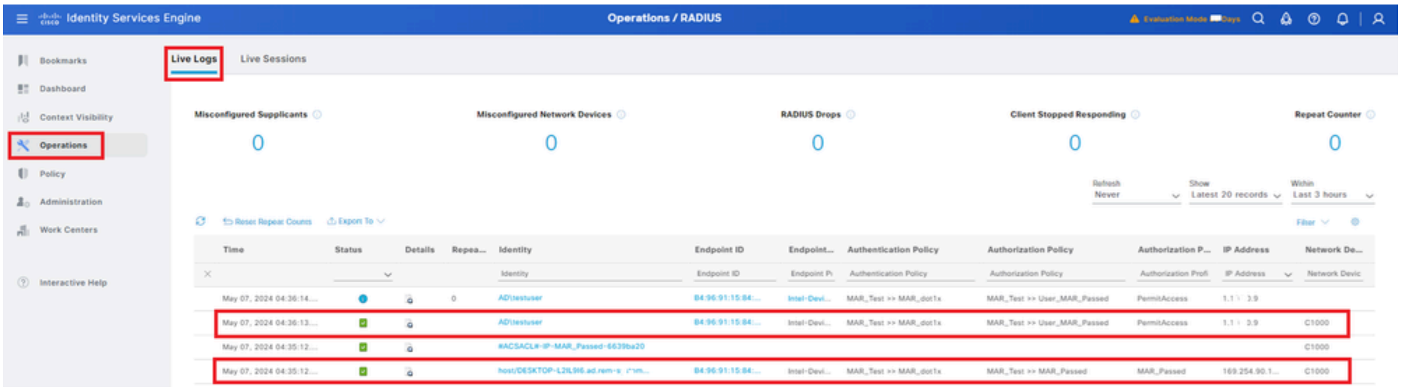
```
AD\testuser
```

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
```

```
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 85s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

步驟 5.確認Radius即時日誌

導航到ISE GUI中的**操作> RADIUS >即時日誌**，確認電腦身份驗證和使用者身份驗證的即時日誌。



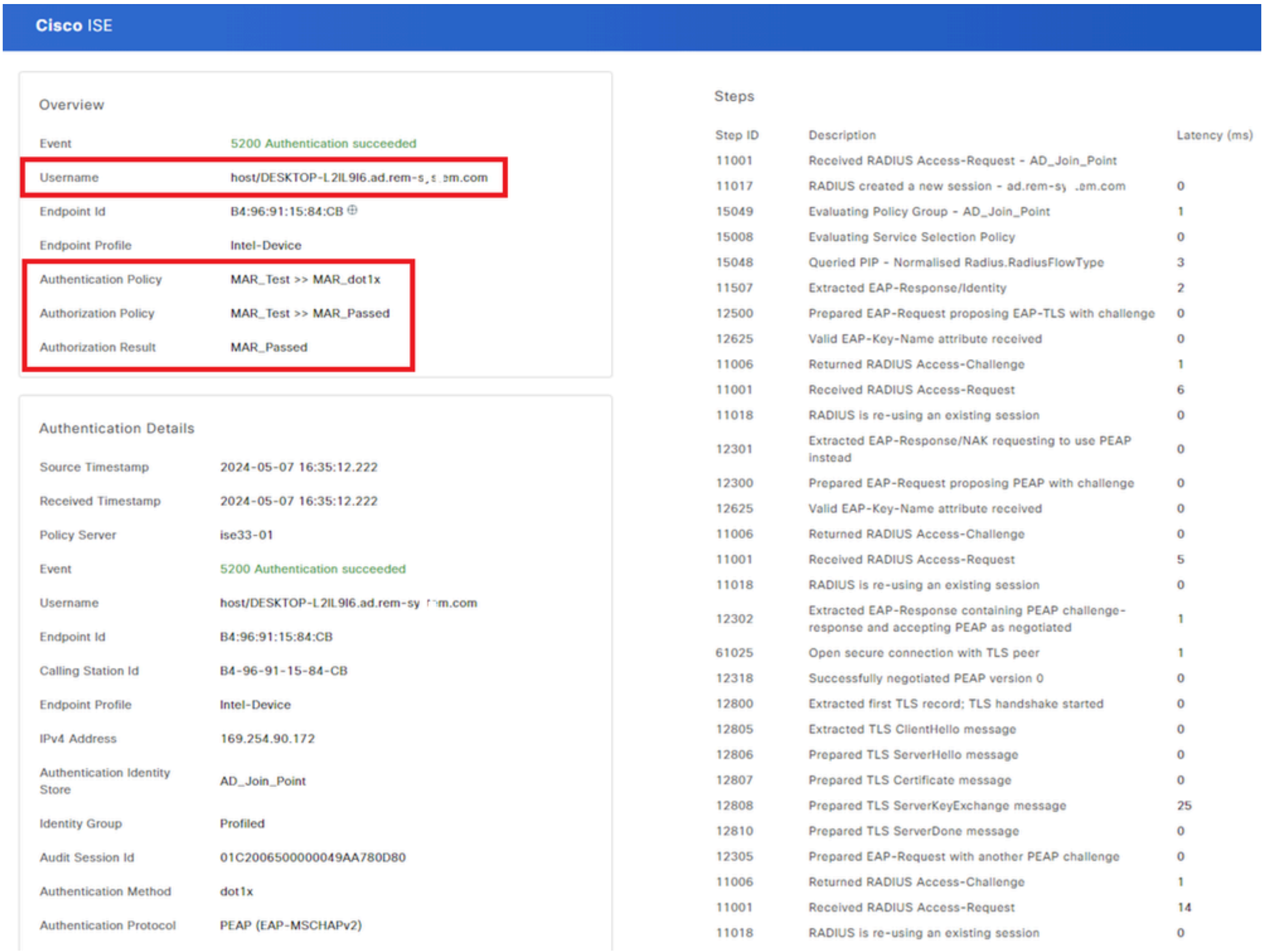
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never　Show: Latest 20 records　Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:36:14....	●		0	AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1 [redacted] 3.9	
May 07, 2024 04:36:13....	✓			AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1 [redacted] 3.9	C1000
May 07, 2024 04:35:12....	✓			#ACSACL#-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12....	✓			host/DESKTOP-L2IL9I6.ad.rem-s [redacted] m...	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

*Radius*即時日誌

確認電腦身份驗證的詳細即時日誌。



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-s,s em.com
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> MAR_Passed
Authorization Result	MAR_Passed

Authentication Details

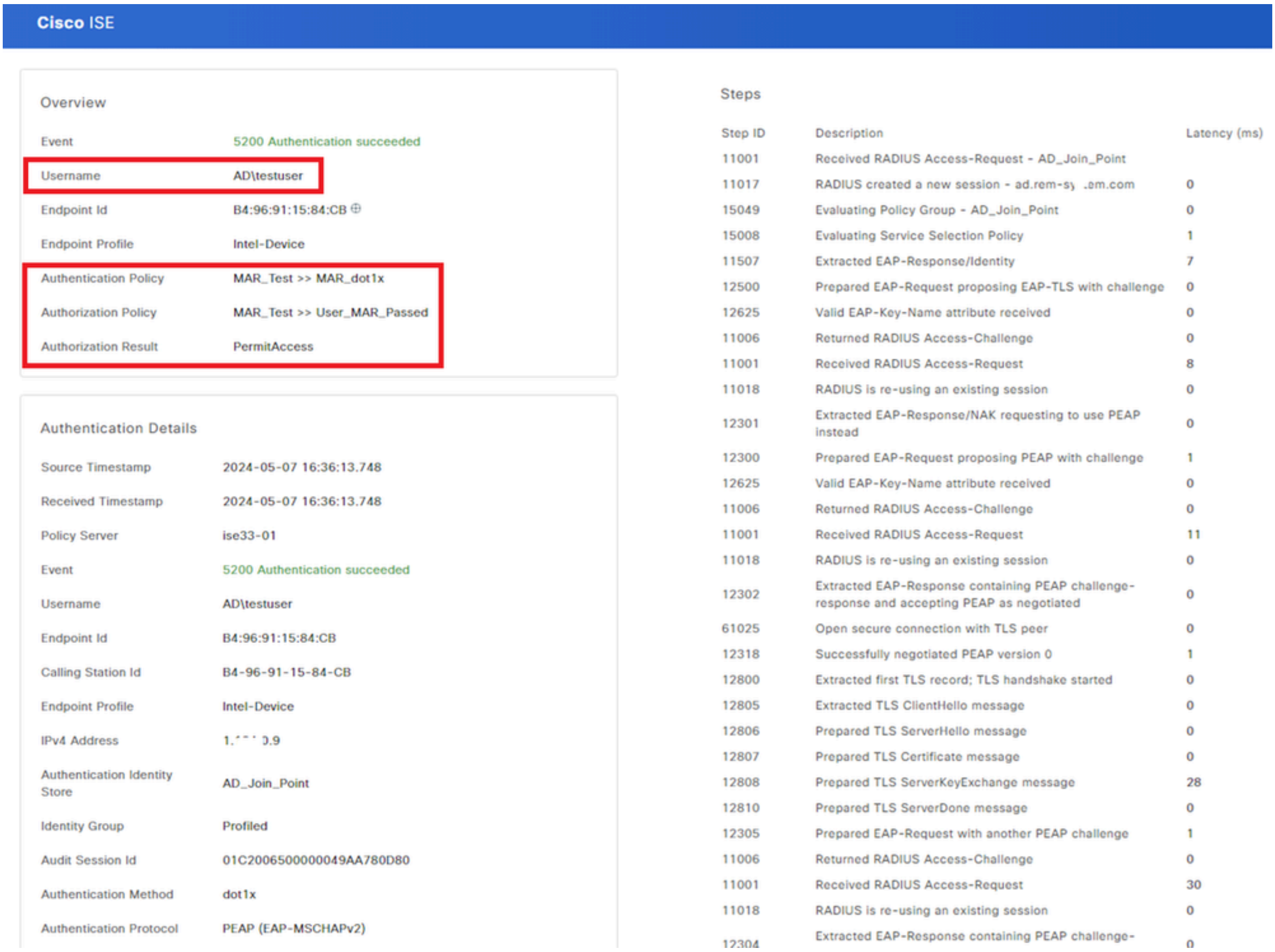
Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy m.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	3
11507	Extracted EAP-Response/Identity	2
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	6
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	25
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0

電腦身份驗證的詳細資訊

確認使用者身份驗證的詳細即時日誌。



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:36:13.748
Received Timestamp	2024-05-07 16:36:13.748
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.[illegible] 0.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy[illegible] .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	0
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	7
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	1
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	11
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	1
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	28
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	1
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	30
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-	0

使用者身份驗證的詳細資訊

模式2.僅限使用者驗證

步驟 1.停用和啟用Windows PC的網絡卡

要觸發使用者身份驗證，請停用並啟用Win10 PC1的NIC。

步驟 2.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/2 details命令以確認C1000中的使用者身份驗證會話。

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

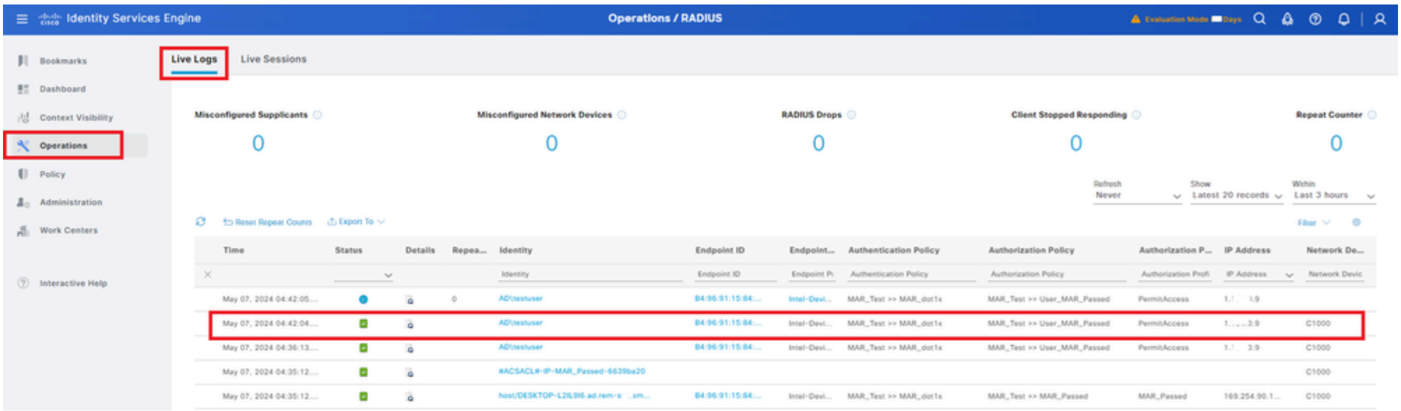
```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name: AD\testuser
```

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

步驟 3.確認Radius即時日誌

在ISE GUI中導航到**操作> RADIUS** >**即時日誌**，確認使用者身份驗證的即時日誌。

注意：由於MAR快取儲存在ISE中，因此僅需要使用者身份驗證。



Misconfigured Supplicants: 0

Misconfigured Network Devices: 0

RADIUS Drops: 0

Client Stopped Responding: 0

Repeat Counter: 0

Refresh: Never

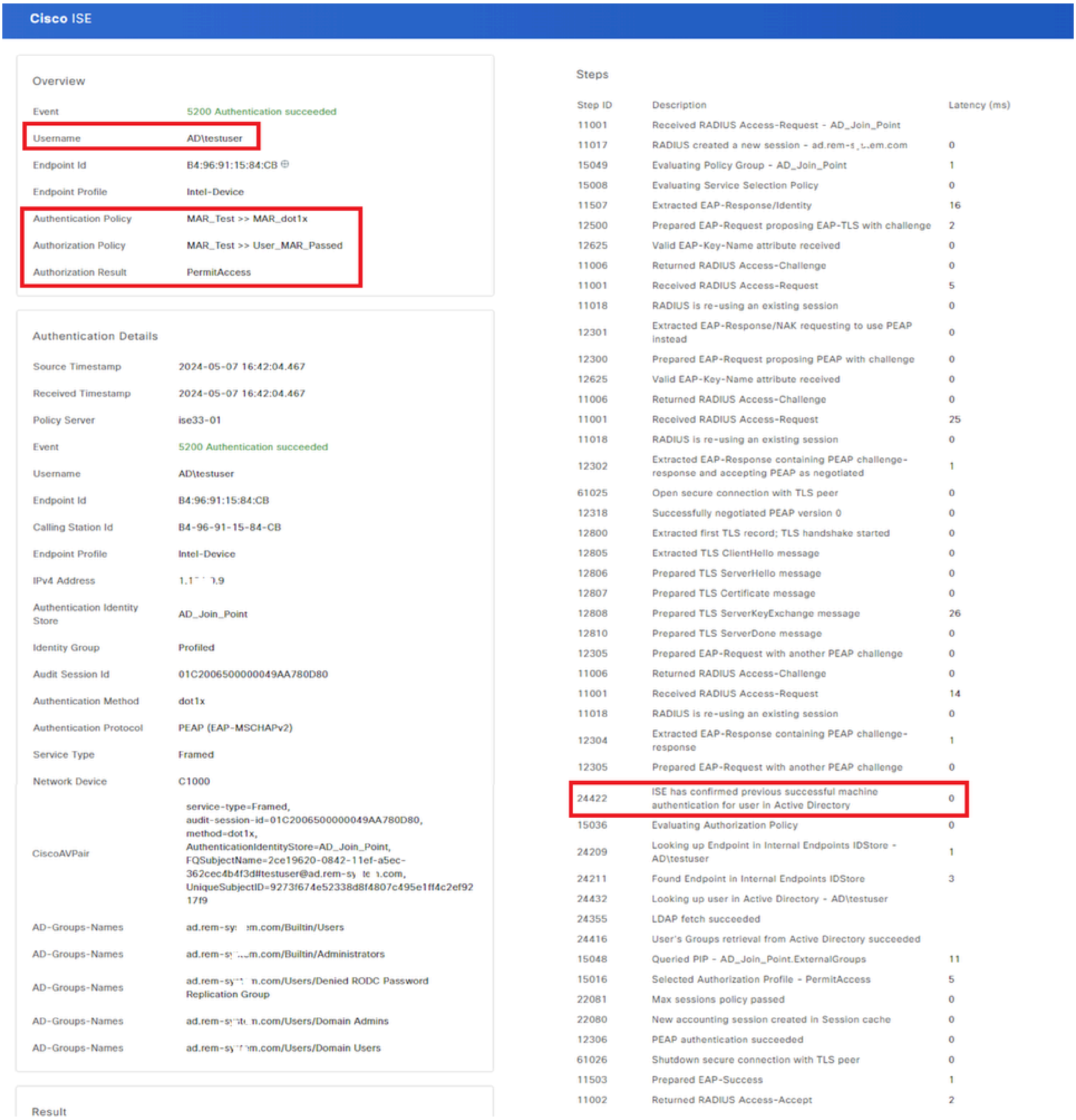
Show: Latest 20 records

Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:42:05....	●	🗎	0	AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.[redacted].9	
May 07, 2024 04:42:04....	✓	🗎		AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.[redacted].9	C1000
May 07, 2024 04:36:13....	✓	🗎		AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.[redacted].9	C1000
May 07, 2024 04:35:12....	✓	🗎		#ACSACL#-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12....	✓	🗎		host/DESKTOP-L2IL9I6.ad.rem-s[redacted]m...	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

*Radius*即時日誌

確認使用者身份驗證的詳細即時日誌。



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:42:04.467
Received Timestamp	2024-05-07 16:42:04.467
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.1˙ ˙).9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	C1000

CiscoAVPair	service-type=Framed,
	audit-session-id=01C2006500000049AA780D80,
	method=dot1x,
	AuthenticationIdentityStore=AD_Join_Point,
	FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d#testuser@ad.rem-sy te 1.com,
	UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9

AD-Groups-Names	ad.rem-sy: :m.com/Builtin/Users
AD-Groups-Names	ad.rem-s...m.com/Builtin/Administrators
AD-Groups-Names	ad.rem-sy n.com/Users/Denied RODC Password Replication Group
AD-Groups-Names	ad.rem-s te n.com/Users/Domain Admins
AD-Groups-Names	ad.rem-sy m.com/Users/Domain Users

Result

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-s .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
11507	Extracted EAP-Response/Identity	16
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	25
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	26
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
24211	Found Endpoint in Internal Endpoints IDStore	3
24432	Looking up user in Active Directory - AD\testuser	
24355	LDAP fetch succeeded	
24416	User's Groups retrieval from Active Directory succeeded	
15048	Queried PIP - AD_Join_Point.ExternalGroups	11
15016	Selected Authorization Profile - PermitAccess	5
22081	Max sessions policy passed	0
22080	New accounting session created in Session cache	0
12306	PEAP authentication succeeded	0
61026	Shutdown secure connection with TLS peer	0
11503	Prepared EAP-Success	1
11002	Returned RADIUS Access-Accept	2

使用者身份驗證的詳細資訊

疑難排解

這些調試日誌(prrt-server.log)可幫助您確認ISE中身份驗證的詳細行為。

- runtime-config

- 執行階段記錄

- runtime-AAA

以下是**模式1**的調試日誌示例。**Machine Authentication和User Authentication**。

<#root>

```
// machine authentication
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

 CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com, IDStore=AD_Join_Point an
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222
MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316
```

相關資訊

電腦存取限制的優缺點

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。